AGENCYWIDE MESSAGE TO ALL NASA EMPLOYEES:

Point of Contact, Valarie Burks, Office of the Chief Information Officer, NASA Headquarters, 202-358-3716, valarie.j.burks@nasa.gov.

MEMORANDUM FOR THE RECORD:

FROM: Charles F. Bolden, Jr., NASA Administrator

Protection of Sensitive Agency Information

This memorandum reinforces NASA policy regarding the protection of Sensitive but Unclassified (SBU) information. The memorandum applies to all Centers, Mission Directorates and their supporting commercial contractors that process NASA information.

Individuals responsible for handling SBU information should be cognizant of the requirements outlined within this memorandum to ensure the protection of all SBU data. SBU information is processed, transported, and maintained in many forms – including on computing devices, removable storage media, fax, copier or multi-function devices, hard copy documents, and voice communications. The protection of the SBU data entrusted to an employee is an individual responsibility. Individuals who travel frequently are reminded to review SBU policies prior to travel to ensure best practices are followed in the protection of SBU data.

It is NASA policy that:

1) All sensitive data at rest (DAR) stored on computing devices (e.g., servers, desktops, laptops, mobile devices) or removable storage media (e.g., thumb drives), shall be encrypted using commercially available encryption technology that, at a minimum, is Federal Information Processing Standard 140-2 (FIPS 140-2) compliant;

2) A mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails, or to support other mission, regulatory, or law enforcement requirements;

3) Sensitive information from external sources labeled For Official Use Only, Controlled Unclassified, or other designations shall be protected according to information owner regulations and policies; and,

4) Written justification shall be provided to the responsible Authorizing Official when appropriate protections are not possible.

For questions regarding SBU or encryption requirements, individuals should consult their Center Chief Information Security Officer (CISO) or Center Privacy Manager. The NASA CIO point of contact for this memorandum is Valarie Burks (202) 358-3716, valarie.j.burks@nasa.gov.

Definitions:

Data at Rest: Includes all data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, cellphones, other removable storage media, hard copy files, video, or other magnetic storage), excluding data that is traversing a firewalled internal NASA network with appropriately established controls, (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

Mobile Computing Devices: Any small hand-held device that provides computing and data storage capabilities (e.g., laptops, BlackBerrys, iPads, and smart phones).

Removable Storage Media: Cartridge and disc-based removable and portable storage media devices that can be used to easily move data between computers (e.g., floppy disks, compact discs, USB flash drives, external hard drives and other flash memory cards/drives that contain non-volatile memory).

Other Portable Data: Information transported by an individual in hard copy, in portfolios, backpacks, brief cases, etc.

This notice is being sent agencywide to all employees by NASA INC in the Office of Communications at NASA Headquarters.